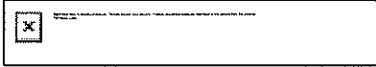


13725  
**Asci, Terry (SCA)**

**From:** noreply@formstack.com  
**Sent:** Monday, October 08, 2018 12:30 PM  
**To:** Breaches, Data (SCA)  
**Subject:** Security Breach Notifications



**Formstack Submission For: Security Breach Notifications - With Uploads**  
**Submitted at 10/08/18 12:29 PM**

**Business Name:** McGlinchey Stafford, PLLC

**Business Address:** 301 Main Street  
Suite 1400  
Baton Rouge, NY 70801

**Foreign Business Address:**

**Company Type:** Other

**Your Name:** Gregory Bautista

**Title:** Attorney

**Contact Address:** Wilson Elser Moskowitz Edelman & Dicker LLP  
1133 Westchester Avenue  
White Plains, NY 10604

**Foreign Contact Address:**

**Telephone Number:** (914) 872-7839

**Extension:**

**Email Address:** gregory.bautista@wilsonelser.com

<b>Relationship to Org:</b>	Other
<b>Breach Type:</b>	Electronic
<b>Date Breach was Discovered:</b>	09/07/2018
<b>Number of Massachusetts Residents Affected:</b>	1
<b>Person responsible for data breach.:</b>	Other
<b>Please give a detailed explanation of how the data breach occurred.:</b>	On September 7, 2018, McGlinchey Stafford, PLLC discovered that individuals' personal information may have been obtained by an unauthorized third party as the result of a phishing attack. After learning that spam emails were sent from an employee's email account to other employees in the firm, McGlinchey Stafford, PLLC immediately engaged computer experts to determine whether information in the account was at risk. The investigation determined that an unknown, unauthorized third party gained access to the employee's account, and could have viewed documents that contained individuals' names and Social Security numbers.
<b>Please select the type of personal information that was included in the breached data.:</b>	Social Security Numbers = Selection(s)
<b>Please check ALL of the boxes that apply to your breach.:</b>	The breach was a result of a malicious/criminal act. = Selection(s)
<b>For breaches involving paper: A lock or security mechanism was used to physically protect the data.:</b>	N/A
<b>Physical access to systems containing personal information was restricted to authorized personnel only.:</b>	Yes
<b>Network configuration of breached system:</b>	Internet Access Available

For breaches involving electronic systems, complete the following:	Personal information stored on the breached system was password-protected and/or restricted by user permissions. = Selection(s)
All Massachusetts residents affected by the breach have been notified of the breach.:	Yes
Method(s) used to notify Massachusetts residents affected by the breach (check all that apply)::	Option2   US Mail
Please explain your answer of Other Above:	
Date notices were first sent to Massachusetts residents (MM/DD/YYYY):	10/08/2018
All Massachusetts residents affected by the breach have been offered complimentary credit monitoring services .:	Yes
Law enforcement has been notified of this data breach.:	No
Please describe how your company responded to the breach. Include what changes were made or may be made to prevent another similar breach from occurring.:	McGlinchey Stafford, PLLC has taken steps to prevent a similar event from occurring in the future, including reviewing and revising their information security policies and resetting employee's access credentials to ensure their systems are secure.
Yes / No:	Yes
File 1 Upload:	View File
File 2 Upload:	
File 3 Upload:	
File - 4 Upload:	

Copyright © 2018 Formstack, LLC. All rights reserved. This is a customer service email.

Formstack, 8604 Allisonville Road, Suite 300, Indianapolis, IN 46250



October 8, 2018

Gregory J. Bautista  
914.872.7839 (direct)  
Gregory.Bautista@wilsonelser.com

**Attorney General Maura Healey**  
Office of the Attorney General  
One Ashburton Place  
Boston, Massachusetts 02108  
ago@state.ma.us

**Undersecretary John C. Chapman**  
Office of Consumer Affairs and Business Regulation  
10 Park Plaza, Suite 5170  
Boston, Massachusetts 02116  
Data.breaches@state.ma.us

Re: Data Security Incident

Dear Attorney General Healey:

We represent McGlinchey Stafford, PLLC with respect to an incident involving the potential exposure of certain personal information described in detail below.

**1. Nature of the possible security breach or unauthorized use or access**

On September 7, 2018, McGlinchey Stafford, PLLC discovered that individuals' personal information may have been obtained by an unauthorized third party as the result of a phishing attack. After learning that spam emails were sent from an employee's email account to other employees in the firm, McGlinchey Stafford, PLLC immediately engaged computer experts to determine whether information in the account was at risk. The investigation determined that an unknown, unauthorized third party gained access to the employee's account, and could have viewed documents that contained individuals' names and Social Security numbers.

**2. Number of Massachusetts residents potentially affected**

Approximately one (1) Massachusetts resident was affected in this potential incident. McGlinchey Stafford, PLLC sent the potentially impacted individual a letter notifying him or her of this incident on October 8, 2018. A copy of the notification sent to the potentially impacted individual is included with this letter, which informs this Massachusetts resident about the 12 months of credit monitoring and identity theft protection services that is being offered to him or her.

1133 Westchester Avenue • White Plains, NY 10604 • p 914.323.7000 • f 914.323.7001

Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston • Indiana • Kentucky  
Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Missouri • New Jersey • New Orleans • New York • Orlando • Philadelphia • Phoenix  
San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

**wilsonelser.com**

**3. Steps McGlinchey Stafford, PLLC has taken or plans to take relating to the potential incident**

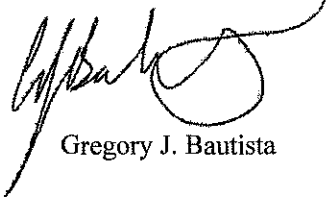
McGlinchey Stafford, PLLC has taken steps to prevent a similar event from occurring in the future, including reviewing and revising their information security policies and resetting employee's access credentials to ensure their systems are secure.

**4. Other notification and contact information**

If you have any additional questions, please contact me at [Gregory.Bautista@wilsonelser.com](mailto:Gregory.Bautista@wilsonelser.com) or (914) 872-7839.

Very truly yours,

**Wilson Elser Moskowitz Edelman & Dicker LLP**



Gregory J. Bautista



C/O ID Experts  
10300 SW Greenburg Rd. Suite 570  
Portland, OR 97223

[First Name] [Last Name]  
[Address 1] [Address 2]  
<<City>>, <<State>> <<Zip>>

To Enroll, Please Call:

800-939-4170

Or Visit:

<https://app.myidcare.com/account-creation/protect>

Enrollment Code:

<<XXXXXXXX>>

10/8/2018

Dear [First Name] [Last Name]:

We are writing to inform you of an incident that may have resulted in the disclosure of your name and Social Security number. As a current or former employee of McGlinchey Stafford PLLC, we take the security of your information very seriously and sincerely apologize for any inconvenience this incident may cause.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. As of September 21, 2018, it is free to freeze and unfreeze your credit file.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax ([www.equifax.com](http://www.equifax.com)); Experian ([www.experian.com](http://www.experian.com)); and TransUnion ([www.transunion.com](http://www.transunion.com)) by regular, certified or overnight mail at the addresses below:

**Equifax Security Freeze**  
P.O. Box 105788  
Atlanta, GA 30348  
[www.freeze.equifax.com](http://www.freeze.equifax.com)  
800-525-6285

**Experian Security Freeze**  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com/freeze](http://www.experian.com/freeze)  
888-397-3742

**TransUnion (FVAD)**  
P.O. Box 2000  
Chester, PA 19022  
[freeze.transunion.com](http://freeze.transunion.com)  
800-680-7289

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.



The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

At this time, there is no indication that your information has been accessed or used by the unauthorized party; however, out of an abundance of caution, we have arranged for you to enroll with ID Experts®, an incident response and recovery services expert, to provide you with MyIDCare™ services at no cost to you. MyIDCare services include:

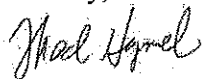
- 12 months Credit Monitoring and CyberScan monitoring;
- \$1,000,000 insurance reimbursement policy;
- Exclusive educational materials; and
- Fully managed Identity Theft Recovery Services (with this protection, MyIDCare will help you resolve issues if your identity is compromised).

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-800-939-4170 or going to <https://app.myidcare.com/account-creation/protect>. Please note the deadline to enroll is January 8, 2019. Please review the *Additional Important Information* on the third and fourth pages of this letter to learn about the additional steps you can take to protect your information at no cost (for example, by asking a consumer reporting agency to place a fraud alert or security freeze on your consumer report information).

We want to assure you that we remain dedicated to protecting your personal information, and are continuing to take steps to prevent a similar event from occurring in the future, including reviewing and revising our policies and resetting employees' access credentials to ensure our systems are secure.

We sincerely regret any inconvenience that this incident may cause you, and remain dedicated to protecting your personal information. Should you have any questions or concerns about this incident, please contact 800-939-4170 Monday through Friday from 6 am - 5 pm Pacific Time or visit <https://app.myidcare.com/account-creation/protect> for more information.

Sincerely,



Thad Hymel  
Chief Information Officer  
McGlinchey Stafford, PLLC



### **Additional Important Information**

**For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina:** It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

---

**For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:**

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com), or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

---

**For residents of Iowa:**

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

---

**For residents of Oregon:**

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

---

**For residents of Maryland, Rhode Island, Illinois, and North Carolina:**

You can obtain information from the Maryland and North Carolina Offices of the Attorneys General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

---

**Maryland Office of the  
Attorney General**

Consumer Protection  
Division  
200 St. Paul Place  
Baltimore, MD 21202  
1-888-743-0023  
[www.oag.state.md.us](http://www.oag.state.md.us)

**Rhode Island Office of  
the Attorney General**

Consumer Protection  
150 South Main Street  
Providence RI 02903  
1-401-274-4400  
[www.riag.ri.gov](http://www.riag.ri.gov)

**North Carolina Office of the  
Attorney General**

Consumer Protection  
Division  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
1-877-566-7226  
[www.ncdoj.com](http://www.ncdoj.com)

**Federal Trade Commission**

Consumer Response Center  
600 Pennsylvania Ave, NW  
Washington, DC 20580  
1-877-IDTHEFT (438-4338)  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

---

**For residents of Massachusetts:** It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

---

**For residents of all states:**

**Fraud Alerts:** You can place fraud alerts with the three credit bureaus by phone and online with Equifax ([https://assets.equifax.com/assets/personal/Fraud\\_Alert\\_Request\\_Form.pdf](https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf)) or Experian (<https://www.experian.com/fraud/center.html>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

**Monitoring:** You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

**Security Freeze:** You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, or regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a freeze. You may obtain a free security freeze by contacting any one or more of the three national consumer reporting agencies:

**Equifax Security Freeze**  
P.O. Box 105788  
Atlanta, GA 30348  
[www.freeze.equifax.com](http://www.freeze.equifax.com)  
800-525-6285

**Experian Security Freeze**  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com/freeze](http://www.experian.com/freeze)  
888-397-3742

**TransUnion (FVAD)**  
P.O. Box 2000  
Chester, PA 19022  
[freeze.transunion.com](http://freeze.transunion.com)  
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

## Asci, Terry (SCA)

---

**From:** Thompson, Bryan <Bryan.Thompson@lewisbrisbois.com>  
**Sent:** Saturday, October 06, 2018 6:18 PM  
**To:** Breaches, Data (SCA)  
**Cc:** McCormick, Simone; Thompson, Bryan; Cunningham, Wendy  
**Subject:** Notice of Security Incident  
**Attachments:** Comfort Inn -- Massachusetts Office of Consumer Affairs and Business Regulation Notification Letter.pdf; Comfort Inn PDX - General Consumer Notification Letter (MA) - template.pdf

Dear Undersecretary Chapman: my firm represents Comfort Inn & Suites Portland Airport ("Comfort Inn"), located in Portland, Oregon. This message is being sent pursuant to Mass. Gen. Laws ch. 93H, §§ 1-6, because on August 27, 2018, Comfort Inn determined the personal information of one (1) Massachusetts resident may be been affected by a data security incident. Comfort Inn notified the affected resident with the attached letter on September 28, 2018. As noted in the attached letters, Comfort Inn is offering the affected resident twelve (12) months of credit monitoring and identity monitoring services through ID Experts. Comfort Inn submitted the Office of Consumer Affairs and Business Regulation's online data breach notification form and provided copies of the attached letters on October 5, 2018. Please contact us should you have any questions. All the best, Bryan



**Bryan M. Thompson, CIPP/US**  
Attorney  
Bryan.Thompson@lewisbrisbois.com  
T: 971.334.7009 F: 971.712.2801

888 SW Fifth Avenue, Suite 900, Portland, OR 97204-2025 | [LewisBrisbois.com](http://LewisBrisbois.com)

**Representing clients from coast to coast. View our locations nationwide.**

This e-mail may contain or attach privileged, confidential or protected information intended only for the use of the intended recipient. If you are not the intended recipient, any review or use of it is strictly prohibited. If you have received this e-mail in error, you are required to notify the sender, then delete this email and any attachment from your computer and any of your electronic devices where the message is stored.